WARD, KEENAN & BARRETT, P.C.
Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Telephone: (602) 279-1717
Facsimile: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

BURSOR & FISHER, P.A.
Neal J. Deckant (*Pro Hac Vice*)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

BURSOR & FISHER, P.A.
Joshua D. Arisohn (*Pro Hac Vice*)
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jarisohn@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Carol Davis, individually and on behalf of all others similarly situated,

Plaintiff,

v.

HDR, Inc.,

Defendant.

Case No. 2:21-cv-01903-SPL

PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS COMPLAINT

TABLE OF CONTENTS

PAGE(S)

TABLE OF AUTHORITIES

PAGE(S)

CASES

STATUTES

Plaintiff Carol Davis ("Plaintiff") respectfully submits this Opposition to Defendant HDR, Inc.'s ("HDR" or "Defendant") Motion to Dismiss the Complaint (ECF No. 11) (the "Motion" or "MTD").

INTRODUCTION

Plaintiff is a long-time member of two private Facebook groups: Ahwatukee411 and Protecting Arizona's Resources & Children (PARC) ("PARC"). Compl. ¶¶ 5-6. Both groups are configured to be private—and have been since their founding—such that "[o]nly members can see who's in the group and what they post."[1] *Id.* ¶¶ 25, 27. Moreover, both groups employ a screening process intended to ensure that the private groups are "only populated with Ahwatukee local[s] [and] PARC members," such that the group members can privately discuss local issues and other topics with likeminded individuals or other residents. *Id.* ¶¶ 24-28.

"Unbeknownst to the Group Members, however, since at least 2016—and going back months if not years earlier—HDR has privately and without consent infiltrated, monitored, wiretapped, and/or accessed posts in the Private Facebook Groups." *Id.* ¶ 29. Defendant is a "multi-billion-dollar architecture and design firm" that also offers a "Strategic Communications" service to clients, which "works to help [HDR's] clients manage the social and political risk associated with infrastructure development." *Id.* ¶ 13. Crucially, Defendant is not a member of the Ahwatukee community, and "PARC … is run by persons who oppose Defendant's interests/projects and the interests/projects of Defendant's clients." *Id.* ¶¶ 7, 28. Thus, neither Defendant nor its employees should have had access to the Private Facebook Groups." *Id.* ¶ 30. Despite this, Defendant snuck its way through both groups' screening processes and, once it had access to the private Facebook groups, analyzed the private posts, "generat[ing] an 'influencer' report, an analysis of public sentiment on social media platforms, and a geospatial analysis that placed communities into categories … The analysis also involve[ed] reading and analyzing the content of the posts in

[1] AHWATUKEE411, https://www.facebook.com/groups/344415615745219/.

the Private Facebook Group for use in the 'comprehensive web-based map.'" *Id.* ¶¶ 13-23, 30-31.[2] Defendant's activities are no different than those of a corporate spy or mole sneaking into a private community to gather intelligence on opponents. And, as Plaintiff alleges, Defendant's activities violated the federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, and constituted an invasion of privacy.

The central premise of Defendant's Motion is that posts in ***private*** Facebook groups are somehow not private. This argument is belied by numerous allegations in the Complaint, as well as caselaw. Compl. ¶¶ 5-6, 24-30, 33; *see also Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659 (D.N.J. 2013) ("The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are configured to be private for purposes of the SCA."). Defendant's other arguments as to the merits of Plaintiff's claims fare no better for the reasons set forth below.

LEGAL STANDARD

"To survive a motion to dismiss, a complaint must contain a short and plain statement of the claim showing that the pleader is entitled to relief such that the defendant is given fair notice of what the [] claim is and the grounds upon which it rests." *White v. Capital One, N.A.*, 2017 WL 11237563, at *1 (D. Ariz. Sept. 29, 2017) (Logan, J.) (internal quotations omitted). "A complaint must state a claim to relief that is plausible on its face.'" *Id.* (internal quotations omitted). "Facial plausibility requires the plaintiff to plead factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

"In deciding a motion to dismiss the Court must accept as true all well-pleaded allegations of material fact, and construe them in the light most favorable to the non-moving party." *Id.* (internal quotations omitted). "In comparison, allegations that are merely

[2] Defendant argues "there is nothing nefarious about reviewing communications from community members in a public forum concerning matters of public concern, such as government works projects." MTD at 2 n.1. The flaw undercutting this argument is that the "forums" at issue were ***private***, not public.

conclusory, unwarranted deductions of fact, or unreasonable inferences are not entitled to the assumption of truth and are insufficient to defeat a motion to dismiss for failure to state a claim." *Id.* (internal quotations and citations omitted). "A plaintiff need not prove the case on the pleadings to survive a motion to dismiss." *Id.* (citing *OSU Student All. v. Ray*, 699 F.3d 1053, 1078 (9th Cir. 2012)).

ARGUMENT

I. PLAINTIFF ADEQUATELY ALLEGES THAT THE FACEBOOK GROUPS WERE PRIVATE

The centerpiece of Defendant's Motion is that "Ms. Davis' claims fail as a matter of law because the Facebook groups at issue are readily accessible to the public and she had no reasonable expectation that her communications would remain private." MTD at 6:15-17. This raises a factual dispute, which must be construed against Defendant at the pleadings stage. *White*, 2017 WL 11237563, at *1. At this stage of the litigation, Plaintiff's well-pled allegations that the Facebook groups were private—allegations the Court must accept as true—should carry the day. *Id.*; Compl. ¶¶ 5-6, 24-30, 33.

Even ignoring this standard, Defendant's argument is still meritless. Defendant "has the burden of proof" as to consent or authorization. *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620 (N.D. Cal. 2021) (noting "the party seeking the benefit of the exception" for consent or authorization under the Wiretap Act and SCA bears the burden of proof). Defendant has not met its burden because its argument is factually and legally incorrect.

A. The Private Facebook Groups Were Private, And Defendant Was Not Authorized To Access The Posts

"[T]he [Wiretap Act] makes clear that the statute's purpose is to protect information that the communicator took steps to keep private." *Ehling*, 961 F. Supp. 2d at 668. Likewise, "[c]ases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information." *Id.*

It is well-established that private posts on social media websites are entitled to protection under the Wiretap Act and SCA. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d

868, 875 (9th Cir. 2002) ("The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and ***private electronic bulletin boards***.") (emphasis added). In *Ehling*, the plaintiff made posts on her "Facebook wall," and limited access to the wall "to only her [300] Facebook friends." *Ehling*, 961 F. Supp. 2d at 662-63. Noting that "the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls," the court held:

> Facebook allows users to select privacy settings for their Facebook walls. Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user. The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are configured to be private for purposes of the SCA.

Id. at 668. "Because Plaintiff in this case chose privacy settings that limited access to her Facebook wall to only her Facebook friends … Plaintiff's Facebook wall posts are covered by the SCA." *Id.* at 669; *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010) ("[T]here is no basis for distinguishing between a restricted-access [bulletin board system ("BBS")] and a user's Facebook wall or MySpace comments.").

The private Facebook groups (and Plaintiff's posts therein) are precisely the types of "restricted-access BBS" that the SCA and Wiretap Act were enacted to protect. As Plaintiff alleges, the Facebook groups are designated as private, meaning "[o]nly members can see who's in the group and what they post."[3] *See* Compl. ¶¶ 25, 27-28. In order to join each group, a prospective group member is required to "fill out a questionnaire," which is intended to ensure that only persons who have a legitimate interest in the groups can join them. *Id.*; *see also Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1322 (11th Cir. 2006) ("[A] short simple statement that the plaintiff screens the registrants before granting access may have been sufficient to infer that the website was not configured to be readily accessible to the general public."). Or, in other words, "[t]he idea of the Private Facebook Groups is that they are private and only populated with Ahwatukee local[s] [and] PARC members, not

[3] AHWATUKEE411, https://www.facebook.com/groups/344415615745219/.

other persons, and certainly not employees or personnel of Defendant." *Id.* ¶ 28; *see also Ehling*, 961 F. Supp. 2d at 669 ("If a BBS was configured to be private, access to the BBS was restricted to a particular community of users, and the messages posted to the BBS were only viewable by those users."); *Lopez v. Apple, Inc.*, 2021 WL 4059106, at *2 (N.D. Cal. Sept. 2, 2021) ("*Lopez II*") (sustaining wiretap claim because although "Apple faults Plaintiffs for not alleging the contents of their communications, [] the private setting alone is enough to show a reasonable expectation of privacy"). Further, the Facebook Terms of Service assured users that others could not access or collect data from its "Products using automated means (without our prior permission) or attempt to access data you do not have permission to access." Compl. ¶ 33. Accordingly, the Facebook groups were private bulletin board systems for members of the Ahwatukee and PARC communities and are thus protected by the Wiretap Act and the SCA.

Similarly, Defendant was not authorized to access the posts in the private Facebook groups and was never given consent to access the posts. *See* 18 U.S.C. § 2701(c)(2) (SCA does not apply to conduct "authorized … by a user of that service with respect to a communication of or intended for that user"); 18 U.S.C. § 2511(2)(c) (Wiretap Act does not apply where "one of the parties to the communication has given prior consent to such interception."). As Plaintiff alleges, "neither Defendant nor its employees should have had access to the Private Facebook Groups." Compl. ¶ 30. As a "Delaware Corporation with is principal place of business … [in] Nebraska" (Compl. ¶ 8), Defendant could not have truthfully claimed a "vested interest in the Ahwatukee community" in order to join the Ahwatukee411 group. *Id.* ¶ 25. And as to PARC, not only was there a survey process, but "the PARC Private Facebook Group is run by persons who ***oppose*** Defendant's interests/projects and the interests/projects of Defendant's clients." Compl. ¶ 28 (emphasis added). Thus, drawing all inferences in Plaintiff's favor—which the Court must do at this stage—the only logical conclusion is that Defendant gained access to the private Facebook groups through deceit and deception. Compl. ¶ 30. And as numerous courts have ruled, such conduct undermines any claim of authorization or consent to view the posts under the

SCA and Wiretap Act respectively. *See, e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) ("Section 2701(c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access … Allowing consent procured by known mistake to serve as a defense would seriously impair the statute's operation."); *Crow v. Uintah Basin Electronic Telecommunications*, 2010 WL 5069852, at *3-4 (D. Utah Dec. 6, 2010) (plaintiff stated an SCA claim where the defendant obtained consent of communication service provider to access text messages through fraud); *Connolly v. Wood-Smith*, 2012 WL 7809099, at *12 (S.D.N.Y. May 14, 2012) (noting that "authorization [] obtained by fraudulent or deceitful conduct" undermines authorization defense to SCA claim).

B. Defendant's Arguments Are Meritless

Defendant raises several arguments as to why the private Facebook groups are not private. Each is without merit.

First, Defendant argues that Plaintiff's communications within the private Facebook groups "were not meaningfully private because no private information was required to access them" and "[a]ny member of the groups could view and disseminate her posts." MTD at 7:22-24. This argument is belied by case law. In *Ehling* and *Crispin*, users did not have to disclose any private information to be friends with the plaintiffs or view the posts, and yet both courts held that the posts were protected by the SCA. *See, e.g.*, *Ehling*, 961 F. Supp. 2d at 662-63 ("Plaintiff selected privacy settings for her account that limited access to her Facebook wall to only her Facebook friends."). As Defendant admits, all that is required is that Plaintiff "configured [her posts] in some way as to limit ready access by the general public." MTD at 7:16-17. Plaintiff did this by posting in private groups where access was limited and posts were viewable only by members of the private groups, and a screening process was necessary to join the groups. Compl. ¶¶ 24-28.[4]

[4] This distinguishes the instant action from *Burke v. New Mexico*, 2018 WL 3054674 (D.N.M. June 20, 2018), which Defendant cites. In *Burke*, the court ruled that a plaintiff's posts on her website were not protected by the SCA because "[p]laintiff registered her webpage in such a way that it could be viewed by any person with a CaringBridge account," as opposed to only people with a CaringBridge account who were specifically given access

Second, citing *Snow*, Defendant argues the private groups were not private because, in order to join the groups, users were only "asked to describe their 'community involvement' and 'interest.'" MTD at 7:28-8:1. But the facts here are a far cry from *Snow*. In *Snow*, all a person had to do to join the group was click a box saying they were not associated with DirecTV. *Snow*, 450 F.3d at 1316; *see also id.* at 1321 ("In sum, to access the electronic bulletin board messages, all one needs to do is register, create a password, and click 'I Agree to these terms.' "). There was no screening process and no checking of whether users were in fact affiliated with DirecTV. By contrast, here, Plaintiff alleges that there was a screening process. Compl. ¶¶ 24-28. The facts here are ***exactly those which*** the court in *Snow* held would be sufficient for protection under the SCA (and the Wiretap Act). *Snow*, 450 F.3d at 1322 ("[A] short simple statement that the plaintiff screens the registrants before granting access may have been sufficient to infer that the website was not configured to be readily accessible to the general public.").

Third, Defendant contends the private groups were not private because "[a]dministrators of the groups have unfettered discretion over access to group communications" and "[a]dministrators can choose not to enforce the nominal requirements they have imposed by automatically granting requests to join the group." MTD at 8:10-13. As an initial matter, the latter argument ("automatically granting requests to join the group") is irrelevant because, as Plaintiff alleges, both groups "have always been private" since their founding. Compl. ¶¶ 25, 27. Thus, the conduct of the group administrators supports Plaintiff's claims because the administrators have maintained the privacy of the Facebook groups since their inception. Further, although the administrators evaluate the results of the screening process to determine who is admitted to the private groups, "[t]he idea of the Private Facebook Groups is that they are private and only populated with Ahwatukee local[s] [and] PARC members, not other persons, and certainly not employees or personnel

---

by plaintiff. *Burke*, 2018 WL 3054674, at *8. That would be akin to a situation where anyone with a Facebook account could view the content on a Facebook group. That is not the case here.

of Defendant." Compl. ¶ 28. And, as noted above, Defendant's access to the groups could only have come through deception or fraud, which is insufficient to support an authorization or consent argument. *Theofel*, 359 F.3d at 1072-73; *Crow*, 2010 WL 5069852, at *3-4. The administrators configured both groups to be private so only group members could view the posts, instituted a screening process to ensure only "Ahwatukee local[s] [and] PARC members" could join the groups (or at least attempted to but for fraud and deception), and maintained those requirements since each group's founding. Compl. ¶¶ 24-28. Each of these allegations supports that the groups are "private electronic bulletin boards" entitled to protection under the SCA and Wiretap Act. *See Ehling*, 961 F. Supp. 2d at 668; *Crispin*, 717 F. Supp. 2d at 969.[5]

Fourth, Defendant argues the groups were not private because "Ms. Davis also had no control over the dissemination of her posts outside the groups themselves." MTD at 8:20-21. This argument goes to whether Defendant was authorized or had consent to view the private posts, not whether the groups were private in the first place. For instance, in *Ehling*, the court ruled that the plaintiff's Facebook wall posts "were covered by the SCA" because the "plaintiff's Facebook page was configured to be private." *Ehling*, 961 F. Supp. 2d at 669. However, the court then ruled that access to the plaintiff's Facebook posts was authorized because the "[p]laintiff's Facebook friend Ronco voluntarily took screenshots of [p]laintiff's Facebook page and either emailed those screenshots to Caruso or printed them out for him." *Id*. In sum, even though authorized Facebook users can share the posts of their friends, the court still ruled the posts were private in the first place before analyzing whether the authorization defense applied. Reversing the order as Defendant insinuates would undermine both statutes, as any conversation on the internet can be shared no matter how private it is.

[5] Here too, Defendant's authorities are distinguishable. *Republic of Gambia v. Facebook, Inc.*, 2021 WL 4304851, at *12 (D.D.C. Sept. 22, 2021) was the "rare case" where "the authors nakedly displayed their intent to reach the public and such intent was independently confirmed." Further, the ruling concerned only public posts, ***not*** private posts. *Id.* ("Thus, ***outside of private messages***, the content requested by The Gambia … falls within the consent exception.") (emphasis added).

Here, however, the facts are significantly different. As illustrated by cases like *Ehling* and *Crispin*, the private Facebook groups were undoubtably private. In contrast to *Ehling* though, Plaintiff has not alleged that Defendant gained access to the private posts by receiving screenshots from legitimate group members. Nor has Defendant demonstrated the same, as is its burden. *Calhoun*, 526 F. Supp. 3d at 620 (noting "the party seeking the benefit of the exception" for consent or authorization under the Wiretap Act and SCA respectively bears the burden of proof). Instead, Defendant gained access to the groups through deception (Compl. ¶¶ 28, 30), which undercuts any claim of authorization or consent. *Theofel*, 359 F.3d at 1072-73; *Crow*, 2010 WL 5069852, at *3-4. Further, Defendant continuously cites Facebook's Terms of Use while ignoring its own violations of them: that users "may not access or collect data from our Products using automated means (without our prior permission) or attempt to access data you do not have permission to access." Compl. ¶ 33; *see also* 18 U.S.C. § 2701(a)(2) (violation of SCA where an entity "intentionally exceeds an authorization to access [a] facility"). Thus, whether the private posts could be disseminated outside of the groups goes to authorization and consent, not privacy in the first place, and Defendant has not demonstrated it had authorization or consent to access the private posts.

Finally, Defendant suggests at several points that the private groups were not private because "Ms. Davis' posts were made to thousands of recipients, many of whom were undoubtedly strangers, and did not implicate her 'private affairs.'" MTD at 14:22-24. But "[p]rivacy protection provided by the SCA does not depend on the number of members in the private Facebook groups." *See Ehling*, 961 F. Supp. 2d at 668. "Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing and would be legally unworkable." *Id.* (quoting *Crispin*, 717 F. Supp. 2d at 990). And far from "strangers," Plaintiff alleges she and other group members believed they were only corresponding with "Ahwatukee local[s] [and] PARC members" (*i.e.*, members of Plaintiff's community). Compl. ¶¶ 24-28.

* * *

In sum, the private Facebook groups qualify for protection under the SCA and Wiretap Act, and Defendant was not authorized to access the private posts.

II. PLAINTIFF SUFFICIENTLY ALLEGES VIOLATIONS OF THE FEDERAL WIRETAP ACT

A. Defendant Unlawfully Intercepted Plaintiff's Private Communications

Defendant advances several unfounded arguments as to why Plaintiff's Wiretap Act claim should be dismissed. ***First***, Defendant argues "by failing to explain 'how or when' HDR became aware of her communications, Ms. Davis has failed to meet her most basic pleading obligations for this claim." MTD at 9:22-23. This is not true. Plaintiff alleges that "since at least 2016—and going back months if not years earlier—HDR has privately and without consent infiltrated, monitored, wiretapped, and/or accessed posts in the Private Facebook Groups." Compl. ¶ 29. Plaintiff further alleges that the wiretapping was conducted using "off-the-shelf tools" that enabled Defendant to "extract, analyze and present demographics, lifestyle patterns and behaviors, and market potential indices." Compl. ¶ 18. And Plaintiff alleges that "neither Defendant nor its employees should have had access to the Private Facebook Groups, nor did the Group Members know Defendant had infiltrated the Private Facebook Groups nor consent to Defendant wiretapping their conversations." Compl. ¶ 30. Although Plaintiff does not know every minute detail of Defendant's wiretapping—nor could she without the benefit of discovery[6]—her allegations are sufficient at this stage to state a claim, and she is not required to plead every detail with specificity at this stage.[7] *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797,

[6] As courts have held in numerous contexts, it is impossible for a plaintiff to know every minute detail without the benefit of discovery. *Reichman v. Poshmark, Inc.*, 267 F. Supp. 3d 1278, 1286 (S.D. Cal. 2017) ("At this stage of the proceeding, it would be unreasonable to require Plaintiff, without the benefit of discovery, to describe the technical details of Defendant's alleged [dialing system]."); *Means v. City of Chicago*, 535 F. Supp. 455, 459 (N.D. Ill. 1982) ("We are at a loss as to how any plaintiff … is supposed to allege with specificity prior to discovery acts to which he or she personally was not exposed, but which provide evidence necessary to sustain the plaintiff's claim.").

[7] *Quigley v. Yelp, Inc.*, 2018 WL 7204066, at *4 (N.D. Cal. Jan. 22, 2018)—which was brought by a *pro se* litigant—is distinguishable because, unlike here, the plaintiff made only

816 (N.D. Cal. 2020) ("[T]he Court rejects Defendants' suggestion that Plaintiffs must identify specific communications that Plaintiffs reasonably believed to be private and that were wrongly recorded. The Court is not convinced that Plaintiffs are required to produce such details at the pleading stage, prior to discovery.").

Second, Defendant argues "there are no well-pleaded allegations establishing that HDR acquired any 'communication' on Ms. Davis' part while it was 'in flight.'" MTD at 10:20-21. This issue is premature at the pleadings stage. *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 841 (N.D. Cal. 2014) ("While Facebook may ultimately produce evidence showing that the messages were actually accessed while in storage, not during transmission, that issue is premature at this stage of the case, and would be better addressed as part of a motion for summary judgment with a more developed factual record."); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028 ("[U]ntil the Court can determine when and how Yahoo intercepted users' emails, the Court must accept as true Plaintiffs' allegation that they were accessed while 'in transit.' Yahoo does not provide the Court with any judicially noticeable information as supporting evidence for its claim that the emails had already reached Yahoo's servers when Yahoo accessed them."). Here, as the factual record is not fully developed, the specifics of when and how the interception occurred will be fleshed out during fact discovery, making this argument premature. At a minimum, if the intended recipients of the posts to the private Facebook groups are other group members, then any interception by Defendant before group members have had an opportunity to read the message would necessarily be *in transit*.

"vague references to 'surveillance systems' and 'surveillance personnel,'" nor did the plaintiff discuss the time of the interception, only that it occurred with no supporting evidence. And in *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1007 (N.D. Cal. 2017), the court dismissed the wiretapping claim against some defendants because the plaintiff "grouped the Defendants together" and the court could not "discern the exact manner in which the other Defendants are alleged to have 'acquired' the contents of an oral communication." By contrast, there is only one defendant here, and Plaintiff has alleged the acquisition of her communications by that Defendant. Compl. ¶¶ 12-23, 31-32.

Third, Defendant argues Ms. Davis fails to describe any device or apparatus HDR purportedly used to acquire her communications. MTD at 10:27-28. Not so. As noted above, Plaintiff alleges how Defendant acquired the communications and what the data was used for. Compl. ¶¶ 13-23, 31. Although Plaintiff does not know the exact name of the software used—which she could not possibly know without discovery—her allegations clearly point to the use of software to extract and analyze postings on a website, are sufficient at this stage to state a violation of the Wiretap Act. *See In re Google Inc. Street View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1082 (N.D. Cal. 2011) (sustaining Wiretap Act claim where "[p]laintiffs plead that Defendant intentionally created, approved of, and installed specially-designed software and technology into its Google Street View vehicles and used this technology to intercept Plaintiffs' data packets, arguably electronic communications, from Plaintiffs' personal Wi–Fi networks").[8]

Finally, Defendant argues that there was no "unlawful" interception because Defendant was an "'intended recipient of … the communication." MTD at 11:16-18. This is false. Again, as the party seeking to establish the consent exception, Defendant "has the burden of proof." *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 685 (N.D. Cal. 2021) ("*Lopez I*") ("Plaintiffs allege that they did not intend Apple to receive their private communications, but that Apple 'captured' such communications using the software in their devices. That sufficiently alleges interception.").[9] Defendant has not met its burden. Defendant merely

[8] In *Rosenow v. Facebook, Inc.*, 2020 WL 1984062, at *7 (S.D. Cal. Apr. 27, 2020)—another *pro se* case—the allegation the court found "conclusory" was the plaintiff's allegation that "Yahoo intercepted Rosenow's communications during transit," not the mention of an algorithm.

[9] The *Lopez I* court also distinguished several of Defendant's authorities. *See Crowley v. CyberSource Corp.*, 165 F. Supp. 2d 1263 (N.D. Cal. 2001); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). Further, contrary to Defendant's arguments about *Lopez I* (MTD at 12:1-5), the court there held the *Guardian* article was not sufficient because the article "does not plausibly suggest that all Apple's devices were subject to accidental triggers," and the plaintiffs did not allege "that their own private communications were intercepted by accidental triggers." *Lopez I*, 519 F. Supp. 3d at 681. By contrast, the *Vice* article does show that interception by the defendant occurred, in what specific private groups it occurred, and what data was collected, and Plaintiff here alleges her private posts were among those intercepted by Defendant. RJN Ex. 4; Compl. ¶¶ 5-6.

speculates how it could have acquired Plaintiff's communications (MTD at 11:12-15), but nothing in Plaintiff's allegations (or Defendant's arguments) supports that Defendant's theory is accurate. In fact, Plaintiff's allegations say the opposite. Compl. ¶¶ 5 ("Plaintiff Davis was unaware at the time that her electronic communications, including the information described above, were being intercepted in real-time and would be disclosed to HDR, nor did Plaintiff Davis consent to the same."); ¶ 29 ("The idea of the Private Facebook Groups is that they are private and only populated with Ahwatukee local PARC members, not other persons, and certainly not employees or personnel of Defendant."); ¶ 30 ("[N]either Defendant nor its employees should have had access to the Private Facebook Groups, nor did the Group Members know Defendant had infiltrated the Private Facebook Groups nor consent to Defendant wiretapping their conversations."); *see also United States v. Eady*, 648 F. App'x 188, 192 (3rd Cir. 2016) ("[A] defendant does not actually participate in a conversation unless his presence is known to the other participants."); *In re Google Inc. Street View Elec. Commc'ns Litig.*, 794 F. Supp. 2d at 1082 ("Plaintiffs plead that the data packets were transmitted over Wi–Fi networks that were configured such that the packets were not readable by the general public without the use of sophisticated packet sniffer technology.").

Thus, Defendant cannot meet its burden to demonstrate that it was a party to Plaintiff's communications with other group members. *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) ("*In re Facebook*") ("[S]imultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception."); *S.D. v. Hytto Ltd.*, 2019 WL 8333519, at *8 (N.D. Cal. May 15, 2019) (no "party" defense where "[a]t no point does that FAC allege that users communicated with Hytto or with the Body Chat app itself"); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) ("[I]t cannot be that anyone who receives a direct signal escapes liability by becoming a party to the communication. Someone who presses up against a door to listen to a conversation is no less an eavesdropper just because the sound waves from the next room reach his ears directly."); *Vasil v. Kiip*,

Inc., 2018 WL 1156328, at *6 (N.D. Ill. Mar. 5, 2018) ("[T]he court can find [] no support for the proposition that a direct, but unintended, recipient of a communication automatically becomes a party to that communication … It is doubtful, to say the least, that the Illinois legislature intended to reward technologically savvy privacy violators by insulating them from liability for unlawful eavesdropping simply because they managed to route the data directly to themselves rather than stealing it from an intended recipient.").

B. Defendant Unlawfully Possessed A Wiretapping Device

Defendant contends that Plaintiff "does not even adequately plead that HDR possessed a wiretap device" and that "the Wiretap Act does not authorize a private cause of action for such conduct." MTD at 12:9-11. This is incorrect. ***First***, Plaintiff alleges Defendant possessed a wiretap device, specifically "commercial off-the-shelf tools to develop powerful applications for communication strategies and issues mapping. These tools enable us to extract, analyze and present demographics, lifestyle patterns and behaviors, and market potential indices." Compl. ¶ 18. This is sufficient at the pleadings stage. *Revitch*, 2019 WL 5485330, at *3 (sustaining claim under analogous California wiretapping statute for possession of wiretap device where "Revitch has [] alleged injuries traceable to Moosejaw's possession and use of the device").

Second, Defendant's argument was rejected by *Luis v. Zang*, 833 F.3d 619 (6th Cir. 2016), where the Sixth Circuit distinguished the same authority Defendant relies upon and noted that in those cases, "the courts were focused on whether a defendant's possession of a wiretapping device, without more, was sufficient to support a private cause of action." *Id.* at 637. By contrast:

> The present case … involves much more than simple possession. Instead, as described above, Awareness allegedly manufactured, marketed, and sold WebWatcher with knowledge that it would be primarily used to illegally intercept electronic communications. ***It then remained actively involved in the operation of WebWatcher by maintaining the servers on which the intercepted communications were later stored for WebWatcher's users***. Awareness thus allegedly took a much more active role in causing the Wiretap Act violation in this case than the defendants in other cases who did nothing more than possess a wiretapping device in contravention of § 2512(1)(b).

Id. at 637 (emphasis added). Thus, a private right of action exists for possession of a wiretap device "when that defendant also plays an active role in the use of the relevant device." *Id*. Here too, Plaintiff alleges that Defendant did far more than merely possess a wiretap device. Plaintiff alleges Defendant was actively involved in the wiretapping process. *See* Compl. ¶¶ 13-23, 29, 31-32, 34. Thus, consistent with *Luis*, Plaintiff has a private right of action under Section 2512 of the Wiretap Act.

III. PLAINTIFF SUFFICIENTLY ALLEGES A VIOLATION OF THE STORED COMMUNICATIONS ACT

In addition to its meritless argument that the private Facebook groups were not private (which is countered above, *see* Argument § I, *supra*), Defendant contends Plaintiff cannot state a violation of the SCA because "Ms. Davis does not identify the means or method by which HDR purportedly accessed communications, or even whether HDR accessed any of her communications." MTD at 13:17-19. Defendant also contends that Plaintiff "fails to offer any facts supporting her allegation that HDR acted 'without authorization.'" MTD at 13:19-20. These arguments are wrong.

First, Plaintiff has alleged that Defendant accessed her posts "[s]ince at least 2016, if not earlier," without authorization and the general topics of these posts. Compl. ¶¶ 5-6. Nothing more is required at the pleadings stage. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 816 ("[T]he Court rejects Defendants' suggestion that Plaintiffs must identify specific communications that Plaintiffs reasonably believed to be private and that were wrongly recorded. The Court is not convinced that Plaintiffs are required to produce such details at the pleading stage, prior to discovery.").

Second, quoting Defendant's own documents, Plaintiff alleges that Defendant accessed the private Facebook groups and used tools to "extract, analyze and present demographics, lifestyle patterns and behaviors, and market potential indices" from the posts therein. Compl. ¶¶ 18, 29, 32; *see also id.* ¶ 31 ("Once Defendant infiltrated the Private Facebook Groups, it generated … an analysis of public sentiment on social media platforms, and a geospatial analysis that placed communities into categories.") (internal quotations

omitted). And, while Plaintiff does not know precisely how Defendant infiltrated the groups—nor could she possibly do so without the benefit of discovery—she does allege that it could have only been through deceit because "neither Defendant nor its employees should have had access to the Private Facebook Groups" due to the objectives of the private groups and criteria for joining them. Compl. ¶¶ 28, 30; *cf. Joe Hand Promotions, Inc. v. Garcia Pacheco*, 2019 WL 2232957, at *1 n.2, *3 (S.D. Cal. May 23, 2019).[10]

Finally, "as the party seeking the benefit of the [authorization] exception," it is Defendant's burden to prove it had authorization to access the private posts. *Calhoun*, 526 F. Supp. 3d at 620. Defendant has not met its burden. *See* Argument § I.A., *supra*.

IV. PLAINTIFF STATES A CLAIM FOR INVASION OF PRIVACY

Defendant argues that Plaintiff's claim for invasion of privacy fails because she "fails to establish 'an intentional intrusion into a private place, conversation or matter,'" because, according to Defendant, "her alleged communications are readily accessible to the public." MTD at 14:5-9. Defendant's argument ignores Plaintiff's allegations that both of the Facebook groups Defendant accessed were private, and required a screening process to gain admission to in order to ensure that only residents "can join the group[s] and are able to see other posts." Compl. ¶¶ 24-28. Thus, contrary to Defendant's say-so, nothing about Plaintiff's communications were "readily accessible to the public." *See Lopez II*, 2021 WL 4059106, at *2 ("[T]he private setting alone is enough to show a reasonable expectation of privacy"); *accord Flanagan v. Flanagan*, 27 Cal. 4th 766, 774-75 (2002).

Defendant also argues Plaintiff cannot show "HDR's purported intrusion into her communications was 'highly offensive.'" MTD at 14:20-21. In *In re Facebook*, 956 F.3d at

[10] Again, Defendant's authorities are off-point. In *Nexsales Corp. v. Salebuild, Inc.*, 2012 WL 216260, at *3 (N.D. Cal. Jan. 24, 2012), unlike here, the plaintiff failed to provide "any factual basis for [its] allegations" that the defendant intentionally accessed the plaintiff's "computer network facility," and even "contradict[ed] its own allegation[s]" of unauthorized access. By contrast, Plaintiff here has alleged and factually supported such intentional access, what was done with the private posts once they were accessed, and that Defendant was not authorized to access the private Facebook groups, she simply has not alleged the precise method by which Defendant infiltrated the groups (which, again, she could not without discovery). Compl. ¶¶ 18, 21, 29-32.

607, the Ninth Circuit held "[t]he ultimate question of whether Facebook's [] practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage." Numerous district courts are in accord. *See In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) ("Considering the quantum and nature of the information collected, the purported failure to respect consumers' privacy choices, and the divergence from the standard industry practice, Plaintiffs plausibly allege Vizio's collection practices amount to a highly offensive intrusion."); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016) ("[T]here is a triable issue of fact regarding whether Yelp's upload of the Plaintiffs' address book data was highly offensive.").

Here, Plaintiff alleges that "Defendant intentionally intruded into conversations in which Plaintiff and members of the Classes had reasonable expectations of privacy. That intrusion occurred in a manner that was highly offensive to a reasonable person. Defendant gained unwanted access to data by electronic and covert means, in violation of the law and social norms." Compl. ¶¶ 84-85. Nothing more is required. *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 130 (3d Cir. 2015) (finding the plaintiffs stated a claim for violation of California's constitutional right to privacy where Google's conduct was "characterized by deceit and disregard … Google's alleged conduct was broad, touching untold millions of internet users; it was surreptitious, surfacing only because of the independent research of Mayer and the Wall Street Journal.").

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' motion in its entirety. If the Court determines that the pleadings are deficient in any respect, Plaintiff requests leave to amend to cure any such deficiencies. *See Roney v. Miller*, 705 F. App'x 670, 671 (9th Cir. 2017) (lower court erred by denying leave to amend after dismissing amended complaint).

Dated: January 28, 2022

Respectfully submitted,

WARD, KEENAN & BARRETT, P.C.

By: */s/ Gerald Barrett*
Gerald Barrett, SBN: 005855
3838 N. Central Avenue, Suite 1720
Phoenix, Arizona 85012
Telephone: (602) 279-1717
Facsimile: (602) 279-8908
E-Mail: gbarrett@wardkeenanbarrett.com

BURSOR & FISHER, P.A.
Neal J. Deckant (*Pro Hac Vice*)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-Mail: ndeckant@bursor.com

BURSOR & FISHER, P.A.
Joshua D. Arisohn (*Pro Hac Vice*)
Alec M. Leslie (*Pro Hac Vice*)
Max S. Roberts (*Pro Hac Vice*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jarisohn@bursor.com
aleslie@bursor.com
mroberts@bursor.com

Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on January 28, 2022, I electronically transmitted the foregoing to the Clerk's office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrants:

William F. Auther
Travis M. Wheeler
BOWMAN AND BROOKE LLP
Suite 1600, Phoenix Plaza
2901 North Central Avenue
Phoenix, Arizona 85012-2736
William.Auther@bowmanandbrooke.com
Travis.Wheeler@bowmanandbrooke.com

John A. Vogt
Ryan D. Ball
JONES DAY
3161 Michelson Drive, Suite 800
Irvine, CA 92612
javogt@jonesday.com
rball@jonesday.com

David M. Morrell
JONES DAY
51 Louisiana Avenue, N.W.
Washington, D.C. 20001
dmorrell@jonesday.com

Attorneys for Defendant HDR, Inc.

By: /s/ Mary Farley